B3

--In U.S. patent no.: 5,661,803; to: Cordery et al.; issued: August 26, 1997, a method for controlling keys used in the verification of encoded information generated by a transaction evidencing device and printed on a document is taught.--

In the claims:

Please rewrite claim 6 as follows:

B4

6. (twice amended) A method as described in claim 10 wherein said message M includes information tying said postage meter's public key Key_{DM}*P to said information IAV.

Please rewrite claim 10 as follows:

10. (amended) A method for certification by a certifying authority of a public key of a digital postage meter, said digital postage meter producing indicia signed with a corresponding private key of said digital postage meter, said certifying authority having a published public key and a corresponding private key, said method comprising the steps of:

B5

a) said certifying authority providing said meter with an integer, said integer being a first function of said private key of said authority;

b) said meter computing a digital postage meter private key as a second function of said integer; and

c) said certifying authority publishing related information; wherein

d) said first function, said second function and said published related information are chosen so that a party seeking to verify said indicia can compute said digital postage meter public key by operating on said published related information with said published public key of said authority.

In response to the Examiner's objection to claim 12 as not easily read at line 8 a clean version of claim 12 is set forth below:

B6

12. A method for certification by a certifying authority of a public key of a digital postage meter, said digital postage meter producing indicia signed with a corresponding private key of said digital postage meter, said certifying authority having a published public key and a corresponding private key, said method comprising the steps of:

a) said certifying authority providing a user with an integer, said integer being a first function of said private key of said authority;

B

b) said user computing a digital postage meter private key as a second function of said integer and downloading said postage meter private key to said digital postage meter ; and

c) said certifying authority publishing related information; wherein

d) said first function, said second function and said published related information are chosen so that a party seeking to verify said indicia can compute said digital postage meter public key by operating on said published related information with said published public key of said authority.

Please cancel claims 25 and 26 and substitute therefore claim 31 as follows:

31. A method of digitally signing a postal indicium comprising the steps of:

a) generating a message m, said message m including indicia data;

b) generating a digital signature with message recovery for said message m; and

c) incorporating said digital signature into said indicium; wherein

d) said generating step further comprises the substeps of:

d1) generating a random integer r_S, $r_S < n$, where n is the order of a group [P] defined on an elliptic curve;

d2) generating a integer K,

$$K = K(r_S * P)$$

where K(p) is a mapping of points in [P] onto the integers, and P is a particular published point in [P];

d3) generating e,

$$e = SKE_K(m)$$

where SKE_K is a symmetric key encryption algorithm using key K;

d4) generating H(M), where H is a hashing function and M is a message which can be recovered from said indicium;

d5) generating $s = Key_{DM}H(M) + r_S$,

where Key_{DM} is the private key of a postage meter which produced said indicium; and

d6) setting said digital signature for said message m equal to the pair (s,e).

Please rewrite claim 27 as follows:

32. (amended) A method as described in claim 31 wherein M = (e,IAV), where IAV is an identity and attributes value for said postage meter.

Please cancel claims 28 and 29 and substitute therefore claim 32 as follows:

24 32. A method of verifying a digital signature of a postal indicium comprising the steps of:

a) recovering a message m from a digital signature of a postal indicium; and

b) accepting said signature as valid if said mesage m is internally consistent; wherein

c)said recovering step further comprises the substeps of:

c1) recovering a public key $Key_{DM}*P$ for a postage meter which produced said indicium;

c2) obtaining the signature (s,e) of said indicium, where $s = Key_{DM}H(M) + r_S$ and $e = SKE_K(m)$, where SKE_K is a symetric key encryption algorithm using key K, m is indicia data, and M is a message recoverable from said indicium;

c3) obtaining M from said indicium;

c4) generating

$$s*P\ [-]\ H(M)Key_{DM}*P =$$
$$H(M)Key_{DM}*P\ [+]\ r_S*P\ [-]\ H(M)Key_{DM}*P =$$
$$r_S*P$$

where [-] is the inverse of [+];

c5) generating

$$K = K(r_S*P)$$

where K(p) is a mapping of points in [P] onto the integers, and P is a particular published point in [P];

c6) generating

$$m = SKE^{-1}{}_K(e)$$

where $SKE^{-1}{}_K$ is the inverse of SKE_K.

Please rewrite claim 30 as follows:

25 30.(amended) A method as described in claim 24 wherein M = (e,IAV), where IAV is an identity and attributes value for said postage meter.